Sentinel 7.3.2 Release Notes

November 2015



Sentinel 7.3.2 improves usability and resolves several previous issues.

Many of these improvements were made in direct response to suggestions from our customers. We thank you for your time and valuable input. We hope you continue to help us ensure that our products meet all your needs. You can post feedback in the Sentinel forum on NetIQ Communities, our online community that also includes product information, blogs, and links to helpful resources.

The documentation for this product is available on the NetIQ website in HTML and PDF formats on a page that does not require you to log in. If you have suggestions for documentation improvements, click **comment on this topic** at the bottom of any page in the HTML version of the documentation posted at the Sentinel NetIQ Documentation page. To download this product, see the Sentinel Product Upgrade website.

1 Software Fixes

The following sections outline software issues resolved in this release:

For the list of software fixes and enhancements in previous releases, see the specific release notes.

1.1 Choosing View Triggers for a Correlation Event in Sentinel Control Center Causes Sentinel Web Interface to Display an Exception

Issue: When a correlation event is linked to an incident, and you select **View Triggers** for that correlation event in Sentinel Control Center (SCC), the Sentinel Web interface displays an exception before displaying events. `(BUG 846198)`

Fix: The Sentinel Web interface now displays the triggers without causing an exception.

1.2 The Sentinel Web Interface Becomes Unresponsive When There Are a Large Number of User Identities

Issue: The Sentinel Web interface becomes unresponsive when there are a large number of user identities to be displayed. `(BUG 895636)`

Fix: Sentinel now displays a fixed number of user identities per search. To narrow down your identities search results, refine your search query by specifying any of the identity parameters in the **Find People** field or use the **Advanced Search** option.

By default, Sentinel displays 500 user identities per search. You can change this value by performing the following steps:

1. Log in to the Sentinel server as the `novell` user.
2. Open the `/etc/opt/novell/sentinel/config/ui-configuration.properties` file.
3. Specify the desired value for the `webui.numberOfIdentitiesToLoad` property.
4. Restart Sentinel.

1.3 The Sentinel Proxy Server Certificate is Overwritten When Accessing Control Center from a Different Sentinel Server

Issue: When you launch SCC from two different Sentinel servers, the Sentinel proxy certificate of the first Sentinel server, which you used to launch SCC, is overwritten with the second Sentinel server proxy certificate. `(BUG 887468)`

Fix: Sentinel now stores the certificates with the IP addresses of the Sentinel servers you use to log in to SCC, and does not prompt for the certificate in those servers where you have already logged in once.

1.4 Synchronization Issue between Sentinel and Sentinel Agent Manager

Issue: When the Sentinel Agent Manager database receives attributes from a large number of agents over a given time period, these attributes are not synchronized to the Sentinel database. `(BUG 926763)`

Fix: Sentinel now has a fine-tuned synchronization mechanism between Sentinel database and Sentinel Agent Manager database.

1.5 Sentinel Does Not Generate Summary Based Reports

Issue: When the maximum event source nodes limit is exceeded, Sentinel does not generate summary based reports, and writes exceptions to log files when you try to run these reports. `(BUG 928211)`

Fix: Sentinel now handles large number of event source nodes efficiently.

1.6 Error When Processing and Storing Event Data

Issue: Sentinel might not process and store event data correctly, if the data buffer locations contain user-created files. `(BUG 930827)`

Fix: Sentinel now deletes all user-created files in the data buffer locations periodically, and processes and stores event data correctly.

1.7 Some Elements in the Sentinel Web Interface Do Not Appear Correctly if the Browser Language is Not English

Issue: If you have set your browser language to a language other than English, some elements in the Sentinel Web interface might not appear correctly. `(BUG 932663 and BUG 940674)`

Fix: Sentinel Web interface displays all the elements correctly in all supported languages.

1.8 Sentinel Displays an Error Message While Logging Out

Issue: If you are using Firefox 37.0.4 or a later version, Sentinel displays an error while logging out. However, there is no impact on the functionality because of this error. `(BUG 935309)`

Fix: Sentinel Web interface handles the logout request correctly and does not display any error while logging out.

1.9 Cannot Delete String Elements from Dynamic Lists

Issue: Sentinel does not let you remove string elements from dynamic lists in SCC or through a correlation action. `(BUG 939244)`

Fix: Sentinel now removes the string elements from the dynamic list files.

1.10 Search Results Are Incomplete for Scheduled Searches in Some Time Ranges

Issue: Search results are incomplete when you perform search with date range by using scheduled saved searches. `(BUG 940604)`

Fix: Sentinel displays the entire search results for saved searches for all time ranges.

1.11 Cannot Edit Scheduled Report Jobs for Reports Created by Using the Create Report Button

Issue: You cannot edit the scheduled report jobs for reports that you created by using **Create Report** in the Sentinel Web interface. Sentinel displays an error message when you try to edit those scheduled report jobs. `(BUG 940785)`

Fix: You can now edit scheduled report jobs for reports you created by using **Create Report** in the Sentinel Web interface.

1.12 Correlation Rules Do Not Support Event Field Names Containing the Underscore Character

Issue: Correlation rules do not allow event fields with names that contain the underscore character (_). `(BUG 940829)`

Fix: Correlation rules allow event fields with names that contain the underscore character.

1.13 Sentinel Overwrites the Custom Configuration Values in server.conf during Upgrade

Issue: During upgrade, Sentinel overwrites the custom configuration values of some properties in the `server.conf` file, such as `wrapper.java.additional.49`. `(BUG 941071)`

Fix: You can now save your custom configuration information by performing the following procedure before the upgrade:

1. Log in to the Sentinel server as the `novell` user and go to the `/etc/opt/novell/sentinel/config/` directory.
2. Create a configuration file named `server-custom.conf` and add your custom configuration parameters in this file.
3. (Optional) Create similar custom configuration files for other components of Sentinel, such as Netflow Collector. For example, `netflow-collector-custom.conf`.

Sentinel applies the saved custom configuration in these configuration files during the upgrade.

1.14 Sentinel Does Not Start After You Upgrade to Version 7.3.1 Because of Complex Correlation Rules

Issue: If lengthy correlation rules with a large number of filter evaluation expressions are available in the deployed state in your Sentinel system before upgrade, Sentinel server, Web interface, and Remote Correlation Engine do not start after you upgrade Sentinel to version 7.3.1.

Also, you cannot create and deploy complex correlation rules in Sentinel 7.3.1. `(BUG 942079)`

Fix: The Sentinel server and other components now start successfully after the upgrade, even if complex correlation rules are present. You can now create and deploy complex correlation rules.

1.15 Sentinel Server Might Shut Down While Running Searches that Span Across a Large Number of Days

Issue: Sentinel server might run out of memory and shut down when you run searches that span across a large number of days, and the number of search results is less than 50000. `(BUG 943943)`

Fix: Sentinel 7.3.2 improves memory utilization during searches that span across a large number of days.

1.16 Data Synchronization Issue between Sentinel and Oracle Database When Event Time is Invalid

Issue: Data synchronization between Sentinel and the Oracle database fails if any event contains invalid date range, for example, a future date such as year 22015. `(BUG 925772)`

Fix: Data synchronization takes place seamlessly. If any events with an invalid date range are encountered, Sentinel logs those events in a log file, and processed with the next batch of events for synchronization.

1.17 Report Generation Process Stops When it Exceeds the Idle Timeout Period

Issue: An idle timeout period with the default value of 15 minutes is configured in Sentinel for report generation process. Often, reports with huge data, such as in an environment where several tenants are present, do not complete in 15 minutes, and report jobs are cancelled abruptly. `(BUG 941612)`

Fix: You can configure the idle timeout period value for report generation by performing the following procedure:

1. Log in to the Sentinel server as the `novell` user.
2. Open the `/etc/opt/novell/sentinel/config/configuration.properties` file.
3. Set a desired value of the `sentinel.report.idle.timeout.mins` property.
4. Restart Sentinel.

1.18 Report Generation Fails When the Report Query Contains the String 'Over'

Issue: The report generation process stops if the report query contains the string `over`. For example, creation of report with the query `(evt:"recovery")` fails. `(BUG 939902)`

Fix: Reports generate correctly even if the report query contains the string `over`.

1.19 Sentinel Logs a Warning Message When Correlation Rules that Depend on a Map Are Deployed on a Remote Correlation Engine

Issue: If you create a correlation rule that depends on a map and deploy it on a remote correlation engine, Sentinel logs the following warning message when the map changes:

```
Received Callback Request for an unregistered Object
```

`(BUG 934765)`

Fix: Sentinel does not log the warning message for correlation rules that depend on a map.

1.20 Refined Event Search Fails after Upgrading to Sentinel 7.3.1

Issue: When you specify a refined event search query in event search, such as `last 30 days`, Sentinel does not display any event data. `(BUG 947867)`

Fix: Sentinel now displays correct data for refined event searches.

1.21 Mappings Created by Using Event Field Mapping Do Not Work after Upgrading to Sentinel 7.3.1

Issue: Mappings created by using event field mapping do not work after you upgrade Sentinel to version 7.3.1. `(BUG 944251)`

Fix: Sentinel regenerates all maps created before upgrade to version 7.3.1, and event mapping works correctly after upgrade to version 7.3.1.

1.22 Solution Designer Displays Null Pointer Exception When You Select Some Correlation Rules from Content Palette

Issue: Solution Designer displays a null pointer exception error when you go to the Content Palette window and select the correlation rules that contain an inlist term that is not surrounded by parentheses. `(BUG 938039)`

Fix: Correlation rules that contain an inlist term that is not surrounded by parentheses are handled properly.

1.23 People Search Does Not Support the Polish Language

Issue: Sentinel fails to display results when you use Polish letters to search in the **People** browser. `(BUG 943261)`

Fix: Sentinel now recognizes the Polish letters in the **People** search and displays results accordingly.

1.24 Sentinel Does Not Display Any Elements in Dynamic Lists after Upgrading to Sentinel 7.3.1

Issue: After you upgrade Sentinel to version 7.3.1, it does not display any list elements in dynamic lists in SCC and the Web interface even though list elements are present in dynamic lists. `(BUG 947622)`

Fix: Sentinel now displays the dynamic list elements in the Web interface and SCC correctly.

1.25 Inconsistent Spacing in the Sentinel Web Interface

Issue: In the Correlation navigation panel, there is inconsistent spacing between the parenthesis and the number that indicates the number of correlation rules. `(BUG 948088)`

Fix: Spacing is now consistent in the Correlation navigation panel.

1.26 Collector Manager Performance Degrades After Upgrading Sentinel to Version 7.3.1

Issue: Changes introduced in Sentinel 7.3.1 to improve the handling of a large number of maps resulted in Collector Manager utilizing significantly more CPU than in previous versions. This may cause the CPU to be overloaded after the upgrade to Sentinel 7.3.1, and the EPS to go down. `(BUG 933409)`

Fix: Mapping service now utilizes considerably less CPU, so the Collector Manager performance is now much closer to the performance of Sentinel versions prior to 7.3.1.

1.27 Sentinel Control Center and Solution Designer Do Not Launch with JRE 8 Update 60

Issue: Sentinel Control Center and Solution Designer do not launch in computers that contain Java version JRE 8 update 60. Sentinel displays the following error:

```
Unable to create trust keystore for web server certificate
```

`(BUG 942290)`

Fix: You can now launch Sentinel Control Center and Solution Designer in computers that contain Java version JRE 8 update 60.

2 System Requirements

For information about hardware requirements, supported operating systems, and browsers, see the Technical Information for Sentinel page.

3 Upgrading to Sentinel 7.3.2

You can upgrade to Sentinel 7.3.2 from Sentinel 7.0 or later.

Download the Sentinel installer from the NetIQ Download website. For information about upgrading to Sentinel 7.3.2, see "Upgrading Sentinel" in the *NetIQ Sentinel Installation and Configuration Guide*.

3.1 Upgrading NetIQ Change Guardian RPM

If you are upgrading Sentinel 7.3 and later, the Change Guardian RPM is not upgraded by default. Therefore, the latest software fixes related to Change Guardian integration are not available. However, integration with Change Guardian works fine post upgrade. You can update the RPM manually. `(BUG 953909)`

To manually update the Change Guardian RPM:

1. Log in as the `root` user and go to the directory where the Sentinel installer is located.
2. Run the following command to check the Change Guardian RPM version bundled in Sentinel:

   ```
   rpm -qa | grep ncgOverlay
   ```
3. Run the following command:

   ```
   rpm -Uvh ncgOverlay-4.1.1.2-1104.i586.rpm
   ```
4. Run the following command to check whether the upgrade is successful:

   ```
   rpm -qa | grep ncgOverlay
   ```

   The output of this command should display the RPM version as 4.1.1.2.

3.2 Post Upgrade Configuration

(Conditional) If you are upgrading to Sentinel 7.3.2 from Sentinel 7.2.2 or older version, perform the following actions:

- After the upgrade, the Search Proxy User role will not have the **Allow users to manage alerts** permission. This permission is necessary for the role to perform remote alert search. Assign the **Allow users to manage alerts** permission to the Search Proxy User role manually.

  For more information, see "Configuring Roles and Users" in the *NetIQ Sentinel Administration Guide*.
- For consistency with newer versions of Sentinel and Sentinel documentation, rename the Search Proxy User role to Data Proxy User after the upgrade.

4 Known Issues

NetIQ Corporation strives to ensure our products provide quality solutions for your enterprise software needs. The following issues are currently being researched. If you need further assistance with any issue, please contact Technical Support.

The Java 8 update and the security vulnerability fixes included in Sentinel 7.3.1 might impact the following plug-ins:

- Cisco SDEE Connector
- SAP Connector
- Remedy Integrator

For any issues with these plug-ins, NetIQ will prioritize and fix the issues according to standard defect-handling policies. For more information about support polices, see Support Policies.

4.1 Cannot Receive Events from Sentinel UNIX Agent 7.4 After Upgrading to Sentinel 7.3.1 and Later

Issue: The security vulnerability fixes included in Sentinel 7.3.1 involved changes to the communication mechanism for a secured connection. These changes are not compatible with Sentinel UNIX Agent 7.4. Therefore, Sentinel cannot receive events from Sentinel UNIX Agent 7.4. `(BUG 953990)`

Workaround: There is no workaround at this time. This issue will be resolved when a compatible version of Sentinel UNIX Agent is made available.

4.2 Cannot View Alerts with IPv6 Data in Alert Views

Issue: Sentinel alert views and alert dashboards do not display alerts that have IPv6 addresses in IP address fields. `(BUG 924874)`

Workaround: To view alerts with IPv6 addresses in Sentinel, perform the steps mentioned in NetIQ Knowledgebase Article 7016555.

4.3 Error When Configuring the NFS Storage After Upgrading Sentinel Appliance to Version 7.3.1 and Later

Issue: Sentinel displays an error when you try to configure NFS as secondary storage location after you Sentinel appliance to version 7.3.1 and later. `(BUG 934851)`

Workaround: After upgrading the Sentinel appliance, restart the SLES operating system using the following command:

```
init 6
```

4.4 Exception in the Sentinel Server Log When You Upgrade Sentinel Versions Prior to 7.3.1 to Versions 7.3.1 and Later

Issue: When you upgrade Sentinel and start the Sentinel server, you might see the following exception in the server log:

```
Invalid length of data object ......
```

`(BUG 933640)`

Workaround: Ignore the exception. There is no impact to Sentinel performance because of this exception.

4.5 Cannot Receive Events from Secure Configuration Manager After Upgrading to Sentinel 7.3.1 and Later

Issue: Sentinel uses the Diffie-Hellman protocol to communicate with Secure Configuration Manager. As part of fixing the Logjam vulnerability, the certificate key size for the Diffie-Hellman protocol in Sentinel has been increased to 2048. However, Secure Configuration Manager uses the default certificate key size; that is, 1024. Because of this mismatch, Secure Configuration Manager can no longer communicate with Sentinel. (BUG 935987)

Workaround: Until a fix is available from Secure Configuration Manager, you can perform the following steps:

WARNING: Performing this workaround overrides the fix for the Logjam vulnerability specified in "Security Vulnerability Fixes" in the *Sentinel 7.3.1 Release Notes*.

---

1. Log in as the `novell` user and open the `/etc/opt/novell/sentinel/config/configuration.properties` file.
2. Comment out the following line following line by prefixing `#`:

   ```
   jdk.tls.ephemeralDHKeySize=2048
   ```
3. Restart Sentinel.

4.6 Cannot Receive Events from Change Guardian After Upgrading to Sentinel 7.3.1 and Later

Issue: As part of fixing the Bar Mitzvah vulnerability, Sentinel disabled the RC4 ciphers on SSL ports enabled for the Web server. However, Change Guardian uses RC4 ciphers to communicate with Sentinel. Therefore, Change Guardian can no longer communicate with Sentinel. (BUG 935401)

Workaround: Until a fix is available from Change Guardian, you can perform the following steps:

WARNING: Performing this workaround overrides the fix for the Bar Mitzvah vulnerability specified in "Security Vulnerability Fixes" in the *Sentinel 7.3.1 Release Notes*.

---

1. Log in as the `novell` user and open the `/etc/opt/novell/sentinel/3rdparty/jetty/jetty-ssl.xml` file.
2. Delete the following lines from the ExcludeCipherSuites list:

   ```
   <Item>SSL_RSA_WITH_RC4_128_SHA</Item>
   <Item>SSL_RSA_WITH_RC4_128_MD5</Item>
   ```
3. Restart Sentinel.
4. Restart the Change Guardian service in the Change Guardian agent computer.

4.7 When Integrated with Change Guardian 4.1, Sentinel Does Not Display Change Guardian Delta Attached Information

Issue: When Sentinel is integrated with Change Guardian 4.1, it does not display Change Guardian delta attached information, in spite of being configured to receive Change Guardian events. (BUG 936704)

Workaround: Upgrade Change Guardian to version 4.1.1 or later.

Or

The Change Guardian Solution Pack 2011.1r4 resolves this issue. Until it is officially released, you can download the Solution Pack from the Sentinel Plug-ins Previews website. You can view the delta information in the following Change Guardian reports after you apply the Solution Pack:

- Change Guardian Events
- Change Guardian Events by Asset
- Change Guardian Events by Policy
- Change Guardian Events by User

4.8 Bar Mitzvah Security Vulnerability in Sentinel Link Connector

Issue: The Bar Mitzvah security vulnerability exists in Sentinel Link Connector. Sentinel Link Connector uses the RC4 algorithm in SSL and TSL protocols, which might allow plaintext recovery attacks against the initial bytes of a stream. For more information, see CVE-2015-2808. (BUG 933741)

Workaround: The Sentinel Link Connector version 2011.1r4 and later resolve this issue. Until it is officially released on the Sentinel Plug-ins website, you can download the Connector from the Previews section.

4.9 The Agent Manager Connector Does Not Set the Connection Mode Property in Events If the Associated Collector Supports Multiple Connection Modes

Issue: The Agent Manager Connector version 2011.1r3 does not set the CONNECTION_MODE property in the events if the Collector parsing the events supports multiple connection modes. (BUG 880564)

Workaround: The Agent Manager Connector version 2011.1r5 and later resolve this issue. Until it is officially released on the Sentinel Plug-ins website, you can download the Connector from the Previews section.

4.10 Sentinel Agent Manager Does Not Consider the RawDataTapFileSize Configuration

Issue: Sentinel Agent Manager ignores the value specified in `RawDataTapFileSize` attribute in the `SMServiceHost.exe.config` file for the raw data file size configuration, and stops writing to the raw data file when the file size reaches 10 MB. (BUG 867954)

Workaround: Manually copy the content of the raw data file into another file and clear it when the file size reaches 10 MB, so that Sentinel Agent Manager can write new data into it.

4.11 Tips Table Search Does Not Return the Complete List of Alert Fields in Upgraded Sentinel Installations

Issue: In upgraded installations of Sentinel 7.3, when you search for alert attributes in the Tips table in the Web interface, the search does not return the complete list of alert fields. However, alert fields display correctly in the Tips table if you clear the search. (BUG 914755)

Workaround: There is no workaround at this time.

4.12 Data Synchronization Fails While Synchronizing IPv6 Addresses in Human Readable Format

Issue: Data synchronization fails when you try to synchronize IPv6 address fields in a human readable format to external databases. For information about configuring Sentinel to populate the IP address fields in human readable dot notation format, see "Creating a Data Synchronization Policy" in the *NetIQ Sentinel Administration Guide*. (BUG 913014)

Workaround: To fix this issue, manually change the maximum size of the IP address fields to at least 46 characters in the target database, and re-synchronize the database.

4.13 Event Search Does Not Respond if You Do Not Have Any Event Viewing Permissions

Issue: If run an event search when your role's security filter is blank and your role does not have event viewing permissions, the search does not complete. The search does not display any error message about the invalid event viewing permissions. (BUG 908666)

Workaround: Update the role with one of the following options:

1. Specify a criteria in the **Only events matching the criteria** field. If users in the role should not see any events, you can enter **NOT sev:[0 TO 5]**.
2. Select **View system events**.
3. Select **View all event data (including raw data and NetFlow data)**.

4.14 The Event fields Panel is Missing in the Schedule Page When Editing Some Saved Searches

Issue: When editing a saved search upgraded from Sentinel 7.2 to a later version, the **Event fields** panel, used to specify output fields in the search report CSV, is missing in the schedule page. (BUG 900293)

Workaround: After upgrading Sentinel, recreate and reschedule the search to view the **Event fields** panel in the schedule page.

4.15 Sentinel Does Not Return Any Correlated Events When You Search for Events for the Deployed Rule with the Default Fire Count Search

Issue: Sentinel does not return any correlated events when you search for all correlated events that were generated after the rule was deployed or enabled, by clicking the icon next to **Fire count** in the **Activity statistics** panel in the Correlation Summary page for the rule. (BUG 912820)

Workaround: Change the value in the **From** field in the Event Search page to a time earlier than the populated time in the field and click **Search** again.

4.16 Sentinel in FIPS 140-2 Mode Does Not Display Change Guardian Delta Attached Information

Issue: Sentinel running in FIPS 140-2 mode does not display Change Guardian delta attached information when you search for Change Guardian events and click the **Change Guardian** icon, in spite of being configured to receive Change Guardian events. Change Guardian releases prior to version 4.2 do not support sending events in FIPS 140-2-compatible mode. (BUG 912230)

Workaround: There is no workaround at this time.

4.17 Data Collection and Data Synchronization With the DB2 Database Fail After Upgrading to Sentinel 7.3

Issue: Upgrading to Sentinel 7.3 causes data collection and data synchronization with the DB2 database to fail, because the upgrade removes the IBM DB2 JDBC driver. (BUG 909343)

Workaround: After upgrading to Sentinel 7.3, add the correct JDBC Driver and configure it for data collection and data synchronization, by performing the following steps:

1. Copy the correct version of the IBM DB2 JDBC driver (`db2jcc-*.jar`) for your version of the DB2 database in the `/opt/novell/sentinel/lib` folder.
2. Ensure that you set the necessary ownership and permissions for the driver file.
3. Configure this driver for data collection. For more information, see the Database Connector documentation.

4.18 New Incoming Alerts Incorrectly Appear to be Selected When You Modify Existing Alerts

Issue: When you click **Select All** in alerts views to select alerts, deselect few alerts, and modify them, new incoming alerts are also selected in the refreshed alert views. This results in wrong count of alerts selected for modification, and also it appears as if you are modifying new incoming alerts too. However, only the originally selected alerts are modified. (BUG 904830)

Workaround: No new alerts will appear in the alert view if you create the alert view with a custom time range.

4.19 Loading Historical Security Intelligence Data Takes a Long Time

Issue: Historical Security Intelligence (SI) data takes a long time to load in Sentinel systems that have a high Events Per Second (EPS) load. (BUG 908599)

Workaround: If you are creating a security intelligence dashboard with historical data, plan to deploy the dashboard when the load on your system is lower, if possible. There is no other workaround at this time.

4.20 Security Intelligence Dashboard Displays Invalid Baseline Duration When Regenerating a Baseline

Issue: During Security Intelligence baseline regeneration, the start and finish dates for the baseline are incorrect and display 1/1/1970. (BUG 912009)

Workaround: The correct dates are updated after the baseline regeneration is complete.

4.21 Sentinel Server Shuts Down When Running a Search If There Are Large Number of Events in a Single Partition

Issue: Sentinel server shuts down when you run a search if there are a large number of events indexed in a single partition. (BUG 913599)

Workaround: Create retention policies in such a way that there are at least two partitions open in a day. Having more than one partition open helps reduce the number of events indexed in partitions.

You can create retention policies that filter events based on the `estzhour` field, which tracks the hour of the day. Therefore, you can create one retention policy with `estzhour:[0 TO 11]` as the filter and another retention policy with `estzhour:[12 TO 23]` as the filter.

For more information, see "Configuring Data Retention Policies" in the *NetIQ Sentinel Administration Guide*.

4.22 Error While Using the report_dev_setup.sh Script to Configure Sentinel Ports for Firewall Exceptions on Upgraded Sentinel Appliance Installations

Issue: Sentinel displays an error when you use the `report_dev_setup.sh` script to configure Sentinel ports for firewall exceptions. `(BUG 914874)`

Workaround: Configure Sentinel ports for firewall exceptions through the following steps:

1. Open the `/etc/sysconfig/SuSEfirewall2` file.
2. Change the following line:

   ```
   FW_SERVICES_EXT_TCP=" 443 8443 4984 22 61616 10013 289 1289 1468 1443
   40000:41000 1290 1099 2000 1024 1590"
   ```

   to

   ```
   FW_SERVICES_EXT_TCP=" 443 8443 4984 22 61616 10013 289 1289 1468 1443
   40000:41000 1290 1099 2000 1024 1590 5432"
   ```
3. Restart Sentinel.

4.23 Sentinel Generic Collector Performance Degrades When Generic Hostname Resolution Service Collector is Enabled

Issue: Sentinel Generic Collector performance degrades when Generic Hostname Resolution Service Collector is enabled on Microsoft Active Directory and Windows Collector. EPS decreases by 50% when remote Collector Managers send events. `(BUG 906715)`

Workaround: There is no workaround at this time.

4.24 Sentinel Cannot Access Security Intelligence, Netflow, and Alert Data in FIPS 140-2 Mode

Issue: When you install Sentinel in FIPS 140-2 mode, connector to Security Intelligence database fails to start, and Sentinel cannot access Security Intelligence, Netflow, and alert data. `(BUG 915241)`

Workaround: Restart Sentinel after installing and configuring in FIPS 140-2 mode.

4.25 Security Intelligence Database and Alert Dashboard Occasionally Do Not Work in Upgraded Custom Installations of FIPS 140-2 Enabled Sentinel

Issue: When you upgrade to Sentinel 7.3 from a custom installation of Sentinel that was installed by a non-root user and was configured in FIPS 140-2 mode, Security Intelligence database and Alert Dashboard occasionally do not start. `(BUG 916285)`

Workaround: Perform the following steps:

1 Go to <*custom installation directory*>/opt/novell/sentinel/bin to know the Sentinel Indexing Service.

2 Run the following command:

```
./si_db.sh status
```

Verify whether the following output displayed:

```
Connection between alert store and indexing service is running.
Security Intelligence database is running.
Indexing service is running.
```

If any of the above mentioned three services are not running, perform the following steps.

3 Run the following command to stop Sentinel:

```
rcsentinel stop
```

4 Log in to the Sentinel server as the `novell` user.

5 Run the following command:

```
<custom installation directory>/opt/novell/sentinel/bin/si_db.sh startnoauth
```

6 Run the following commands to add dbauser and appuser users:

```
cd <custom installation directory>/opt/novell/sentinel/3rdparty/mongodb/bin
./mongo
use admin
db.addUser ("dbauser", "novell")
use analytics
db.addUser ("appuser", "novell")
exit
```

7 Stop the MongoDB database:

```
<custom installation directory>/opt/novell/sentinel/bin/si_db.sh stop
```

8 Perform the following steps to add encrypted password fields:

8a Run the following command to get the encrypted password for the `novell` user:

```
<custom installation directory>/opt/novell/sentinel/bin/encryptpwd -e
novell
```

Encrypted password is displayed. For example:

```
bVWOzu6okMmMCkgM0aHeQ==
```

8b In the `configuration.properties` file, update the `baselining.sidb.password` and `baselining.sidb.dbpassword` properties with the encrypted

password. for example:

```
baselining.sidb.password=9bVWOzu6okMmMCkgM0aHeQ==
baselining.sidb.dbpassword=9bVWOzu6okMmMCkgM0aHeQ==
```

9 Exit from the `novell` user account and start Sentinel as root user using the following command:

```
rcsentinel start
```

NOTE: Run the `configure.sh` script to reset the password whenever needed. For more information about running the `configure.sh` script, see "Modifying the Configuration after Installation" in the *NetIQ Sentinel Installation and Configuration Guide*.

4.26 Sentinel Does Not Configure the Sentinel Appliance Network Interface By Default

Issue: When installing Sentinel Appliance, the network interface is not configured by default. (BUG 867013)

Workaround: To configure the network Interface:

1. In the Network Configuration page, click **Network Interfaces**.
2. Select the network interface and click **Edit**.
3. Select **Dynamic Address** and then select either **DHCP** or **Static assigned IP Address**.
4. Click **Next** and then **OK**.

4.27 The Web Browser Displays an Error When Exporting Search Results in Sentinel

Issue: When exporting search results in Sentinel, the Web browser might display an error if you modify the operating system language settings. (BUG 834874)

Workaround: To export search results properly, perform either of the following:

- While exporting the search results, remove any special characters (outside the ASCII characters) from the export filename.
- Enable UTF-8 in the operating system language settings, restart the machine, and then restart the Sentinel server.

4.28 Partitions Removed from Secondary Storage are Also Removed from Primary Storage

Issue: If the number of days of data that secondary storage can hold is less than the number of days of data that primary storage holds, Sentinel does not use the disk space in primary storage efficiently. Partitions removed from secondary storage to free up space will also be removed from primary storage. (BUG 860888)

Workaround: Allocate enough space in secondary storage to hold data for the total number of days you want to keep online (searchable).

For more information, see “Event Data” in the *NetIQ Sentinel Administration Guide*.

4.29 Sentinel Services Might Not Start Automatically After the Installation

Issue: On systems with more than 2 TB disk space, Sentinel might not start automatically after the installation. (BUG 846296)

Workaround: As a one-time activity, start the Sentinel services manually by specifying the following command:

```
rcsentinel start
```

4.30 Cannot Enable Kerberos Authentication in Sentinel Appliance Installations

Issue: In Sentinel appliance installations, if you configure Kerberos authentication in the Kerberos module, the console displays a confirmation message that the Kerberos client configuration was successful. When you view the Kerberos module again, however, the **Enable Kerberos Authentication** option is deselected. `(BUG 843623)`

Workaround: There is no workaround at this time.

4.31 Unable to Install the Remote Collector Manager If the Password Contains Special Characters

Issue: When you install a remote Collector Manager, if you specify a password that contains special characters, such as '$', '"', '\', or '/', the installation fails with errors. `(BUG 812111)`

Workaround: Do not use special characters in the remote Collector Manager password.

4.32 Restarting a Remote Collector Manager Causes Some Event Sources to Lose Connection

Issue: When you restart a remote Collector Manager appliance, the Syslog event sources connected on the UDP port lose connection. `(BUG 795057)`

Workaround: There is no workaround available at this time.

4.33 Unable to View More Than One Report Result at a Time

Issue: While you wait for one report result PDF to open, particularly report results of 1 million events, if you click another report result PDF to view, the report result is not displayed. `(BUG 804683)`

Workaround: Click the second report result PDF again to view the report result.

4.34 Agent Manager Requires SQL Authentication When FIPS 140-2 Mode is Enabled

Issue: When FIPS 140-2 mode is enabled in your Sentinel environment, using Windows authentication for Agent Manager causes synchronization with the Agent Manager database to fail. `(BUG 814452)`

Workaround: Use SQL authentication for Agent Manager when FIPS 140-2 mode is enabled in your Sentinel environment.

4.35 Sentinel High Availability Installation in FIPS 140-2 Mode Displays an Error

Issue: If FIPS 140-2 mode is enabled, the Sentinel High Availability installation displays the following error:

```
Sentinel server configuration.properties file is not correct. Check the
configuration file and then run the convert_to_fips.sh script again to enable FIPS
mode in Sentinel server.
```

However, the installation completes successfully. (BUG 817828)

Workaround: There is no fix or workaround available at this time. Although the installer displays the error, the Sentinel High Availability configuration works successfully in FIPS 140-2 mode.

4.36 Sentinel High Availability Installation in Non-FIPS 140-2 Mode Displays an Error

Issue: The Sentinel High Availability installation in non-FIPS 140-2 mode completes successfully but displays the following error twice:

```
/opt/novell/sentinel/setup/configure.sh: line 1045: [: too many arguments
```

(BUG 810764)

Workaround: There is no fix or workaround available at this time. Although the installer displays the error, the Sentinel High Availability configuration works successfully in non-FIPS 140-2 mode.

4.37 Appliance Update From Versions Prior to Sentinel 7.2 Fails in WebYaST

Issue: Appliance update from versions prior to Sentinel 7.2 fails because the vendor for the update packages has changed from Novell to NetIQ. (BUG 780969)

Workaround: Use the zypper command to upgrade the appliance. For more information, see "Upgrading the Appliance by Using zypper" in the *NetIQ Sentinel Installation and Configuration Guide*.

4.38 Error While Installing Correlation Rules

Issue: Solution Manager does not install correlation rules when a correlation rule with an identical name already exists on the system. A `NullPointerException` error is logged in the console. (BUG 713962)

Workaround: Ensure that all correlation rules have a unique name.

4.39 Sentinel Link Action Displays Incorrect Message

Issue: When you execute a Sentinel Link action from the Web interface Sentinel displays a success message even though the Sentinel Link Connector integrator test failed from the Sentinel Control Center. (BUG 710305)

Workaround: There is no workaround at this time.

4.40 Dashboard and Anomaly Definitions with Identical Names

Issue: When a Security Intelligence dashboard and an anomaly definition have identical names, the dashboard link is disabled on the Anomaly Details page. (BUG 715986)

Workaround: Ensure you use unique names when creating dashboards and anomaly definitions.

4.41 Active Search Jobs Duration and Accessed Columns Inaccuracies

Issue: The Sentinel Web interface displays negative numbers in the Active Search Job Duration and Accessed columns when the Sentinel Web interface computer clock is behind the Sentinel server clock. For example, the Duration and Accessed columns display negative numbers when the Sentinel Web interface clock is set to 1:30 PM and the Sentinel server clock is set to 2:30 PM. `(BUG 719875)`

Workaround: Ensure the time on the computer you use to access the Sentinel Web interface is the same as or later than the time on the Sentinel server computer.

4.42 IssueSAMLToken Audit Event Displays Incorrect Information in the Security Intelligence Dashboard

Issue: When you log in to the security dashboard and perform a search for `IssueSAMLToken` audit event, the `IssueSAMLToken` audit event displays incorrect hostname (InitiatorUserName) or (IP address) SourceIP. `(BUG 870609)`

Workaround: There is no workaround at this time.

4.43 Sentinel Control Center Does Not Launch When NetIQ Identity Manager Designer is Installed on the Client Computer

Issue: Sentinel Control Center does not launch when the NetIQ Identity Manager Designer is installed on the client computer and Designer uses the system JRE. Designer needs to add some supporting jar files like `xml-apis.jar` to the `lib/endorsed` directory. Some of the classes in the `xml-apis.jar` file override the corresponding classes in the system JRE that is used by the Sentinel Control Center. `(BUG 888085)`

Workaround: Configure Designer to use its own JRE.

4.44 Sentinel Agent Manager Does Not Capture the Windows Insertion String Fields With Null Values

Issue: While collecting event data, Sentinel Agent Manager does not capture the Windows Insertion String fields with null values. `(BUG 838825)`

Workaround: There is no workaround at this time.

5 Contact Information

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, please email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

For detailed contact information, see the Support Contact Information website.

For general corporate and product information, see the NetIQ Corporate website.

For interactive conversations with your peers and NetIQ experts, become an active member of our community. The NetIQ online community provides product information, useful links to helpful resources, blogs, and social media channels.

6 Legal Notice

NetIQ Sentinel is protected by United States Patent No(s): 05829001.